BAILEY & GLASSER, LLP
Arthur H. Bryant (State Bar No. 208365)
abryant@baileyglasser.com
1999 Harrison Street, Suite 660
Oakland, CA 94612
(304) 345-6555 (main) / (304) 342-1110 (fax)

John W. Barrett (*admitted pro hac vice*)
jbarrett@baileyglasser.com
209 Capitol Street
Charleston, WV 25301
(304) 345-6555 / (304) 342-1110 (fax)

THE GOLAN FIRM PLLC
Yvette Golan (*admitted pro hac vice*)
y.golan@tgfirm.com
529 14th Street NW Suite 914
Washington, DC 20045
(866) 298-4150 / (928) 441-8250 (fax)

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

FRANK D. RUSSO, KOONAN LITIGATION CONSULTING, LLC, and SUMNER M. DAVENPORT & ASSOCIATES, LLC, on behalf of a similarly situated class, Plaintiff, vs. MICROSOFT CORPORATION, Defendant.	Case No. 3: 20-CV-04818-YGR **AMENDED COMPLAINT** **CLASS ACTION** **DEMAND FOR JURY TRIAL** Honorable Yvonne Gonzalez Rogers

Table of Contents

SUMMARY OF CLAIMS

1. This is a national class action against Microsoft for misrepresenting its privacy and security practices, violating federal and state law, and illegally sharing and using its business-class Microsoft Office 365 and Microsoft Exchange customers' data.[1] Contrary to Microsoft's representations and without its customers' consent, Microsoft shares the Plaintiffs' and all other business customers' contacts and related data with Facebook; shares their other data with unauthorized third parties for unauthorized purposes; and uses the content of their emails, documents, contacts, calendars, and other data to develop new products and services to sell to others. Those actions violate the Wiretap Act, 18 U.S.C. § 2511; the Stored Communications Act, 18 U.S.C. § 2702; and the consumer protection and privacy laws of Washington.

INTRODUCTION

2. Businesses require privacy and security to protect their data, which includes sensitive information belonging to them, their employees, their customers or clients, confidential business plans and financial projections, and trade secrets.

3. Knowing that business customers would be wary of transitioning to the cloud, Defendant Microsoft Corporation has made privacy, security, transparency, and trust the core themes of its marketing efforts for its phenomenally successful Office 365 (now called Microsoft 365) and Exchange Online services.[2] Like a mantra, Microsoft has repeatedly promised business customers that it will use their content and data exclusively to provide them with the purchased services; that, solely for those purposes, it will share their data with its subcontractors and certain

[1] When used in this Complaint, unless the context suggests otherwise, "businesses," "business customers," and similar terms include persons and non-governmental entities, including non-profit organizations, that subscribe to or purchase business-class versions of Microsoft Office 365 and Microsoft Exchange, as specified in the class definition at ¶ 140, *infra*. Because these business-class versions are exclusively cloud-based, all "business customers" are cloud-software customers of Microsoft. For that reason, when Plaintiffs allege that Microsoft shared and used the data of each Plaintiff and business customers as described below, Microsoft's sharing and usage practices affect all cloud-software business customers.

[2] On April 21, 2020, Office 365 became Microsoft 365. All references to Office 365 in this Complaint include references to Microsoft 365 as of that date and thereafter.

others only on a need-to-know basis; and that it will never share the customer's data with third parties at all.

4. In fact, with respect to each Plaintiff and all business customers who use the cloud-software products specified in the class definition:

a. Contrary to its representations, Microsoft shared the Plaintiffs' and class members' contact data with third parties including Facebook without consent, even when sharing was not necessary to provide the purchased services (Part C.1., *infra)*;

b. Contrary to its representations, Microsoft itself used Plaintiffs' and class members' authentication, email, document, task, and contact data to develop and sell new products and services to others (Part C.2, *infra*); and

c. Microsoft misrepresents the security it provides for business customer data by falsely promising that it complies with privacy and confidentiality standards known as "SOC" standards (Part C.3, *infra*). [3]

5. Microsoft's practices violate federal laws governing the acquisition, use, and sharing of electronic communications; state laws prohibiting deceptive advertising and unfair acts and practices; and state privacy laws.

6. Plaintiffs bring this lawsuit to hold Microsoft accountable, expose and stop its illegal conduct, and obtain compensation for all Office 365 and Exchange Online business customers in America who paid for services and products that were not as Microsoft claimed.

PARTIES AND PLAINTIFF-SPECIFIC ALLEGATIONS

7. Plaintiffs Frank D. Russo, Koonan Litigation Consulting, LLC, and Sumner M. Davenport & Associates, LLC are persons or companies that have subscribed to or purchased business versions of Microsoft's services and products, as specified below. All Plaintiffs accessed these Microsoft services through the cloud. They seek to represent a nationwide class of

[3] Unless specifically noted otherwise or made clear by the context, all conduct alleged in this Complaint has taken place throughout the Class Period and is still taking place.

similarly situated Microsoft business customers, who all accessed these services through the cloud. All Plaintiffs' and all Microsoft's business customers' data has been improperly shared, improperly used, and improperly secured, as alleged below.

8. Defendant Microsoft Corporation is a Washington corporation headquartered in Redmond.

Factual Allegations Regarding Plaintiff Russo

9. Plaintiff Frank D. Russo resides in Napa, California. He operates a sole proprietorship called Russo Mediation & Law, which provides mediation, arbitration, and alternative dispute resolution services to bring parties from conflict to resolution by establishing rapport, earning trust, understanding perspectives, and overcoming legal, psychological, and philosophical differences.

10. Since August 2015, Plaintiff Russo has paid approximately $12.50 per month for his subscription to Microsoft 365 Business Standard (formerly called "Office 365 Business Premium").

11. At all times, Microsoft 365 Business Standard was a cloud-based software platform.

12. Plaintiff Russo is a regular user of Office 365 (including its Outlook functions – in particular, its email, calendar, and contacts functions) in the course of his business, and in the course of his personal affairs. Plaintiff Russo also regularly uses Office 365's document functions.

13. The privacy and security of Plaintiff Russo's and his clients' data are important and material to him.

14. In deciding to subscribe to Office 365, Plaintiff Russo believed Microsoft would keep Plaintiff Russo's data private and secure.

15. Microsoft misrepresented and did not disclose to Plaintiff Russo material facts, alleged more specifically below, regarding its use and protection of Plaintiff Russo's data, and, as a result, Plaintiff Russo was deceived. Had Microsoft not made these misrepresentations and

had it properly disclosed these facts, Plaintiff Russo would not have purchased his subscription, or alternatively would have paid less for it.

16. Plaintiff Russo has started exploring what actions he can take, other than filing this lawsuit, to protect himself from the actions by Microsoft described in this Complaint.

Factual Allegations Regarding Plaintiff Koonan

17. Plaintiff Koonan Litigation Consulting, LLC ("Plaintiff Koonan") is a California limited liability corporation headquartered in San Francisco, doing business with another company as Chopra Koonan Litigation Services.

18. Plaintiff Koonan provides its clients with advice on how to succeed in all aspects of litigation, including with case analysis, theme development, focus groups, mock trials, witness preparation, opening statements, closing arguments, jury selection, and post-trial juror interviews.

19. Since February 2016, Plaintiff Koonan has paid approximately $119.88 annually for its subscription to Microsoft 365 Business Basic (formerly called "Office 365 Business Essentials").

20. At all times, Microsoft 365 Business Basic was a cloud-based software platform.

21. Plaintiff Koonan is a regular user of Office 365 (including its Outlook functions – in particular, its email, calendar, and contacts functions) in the course of its business. Plaintiff Koonan also regularly uses Office 365's document functions.

22. The privacy and security of Plaintiff Koonan's and its clients' data are important and material to it.

23. In deciding to subscribe to Office 365, Plaintiff Koonan believed Microsoft would keep Plaintiff Koonan's data private and secure.

24. Microsoft misrepresented and did not disclose to Plaintiff Koonan material facts, alleged more specifically below, regarding its use and protection of Plaintiff Koonan's data, and, as a result, Plaintiff Koonan was deceived. Had Microsoft not made these misrepresentations and had it properly disclosed these facts, Plaintiff Koonan would not have purchased its subscription, or alternatively would have paid less for it.

25. Plaintiff Koonan has started exploring what action it can take, other than filing this lawsuit, to protect itself from the actions by Microsoft described in this Complaint.

Factual Allegations Regarding Plaintiff Davenport

26. Plaintiff Sumner M. Davenport & Associates, LLC ("Plaintiff Davenport"), is a Wyoming limited liability corporation. Plaintiff Davenport's primary place of business is in Woodland Hills, CA. Sumner Davenport is a California resident and has been throughout the class period. Plaintiff Davenport is a marketing company that works with small businesses, and charitable organizations on web accessibility, communication strategies, digital and print marketing, reputation management, and research. Plaintiff Davenport serves clients throughout Southern California.

27. Since 2016, Plaintiff Davenport has subscribed to Microsoft 365 Business Standard (formerly called "Office 365 Business Premium").

28. From approximately April 2016 through April 2018, Plaintiff Davenport paid $12.50 per month for its Microsoft 365 Business Standard account.

29. From approximately April 2018 through the present, Plaintiff Davenport paid an annual subscription fee of $150 for the Microsoft 365 Business Standard account.

30. At all times, Microsoft 365 Business Standard was a cloud-based software platform.

31. Plaintiff Davenport purchased its subscription to Office 365 online.

32. Before purchasing Office 365, Plaintiff Davenport's principal, Sumner Davenport, conducted online research to identify the best solution for its document management, backup, and other business needs.

33. Plaintiff Davenport is a regular user of Office 365 (including its Outlook functions – in particular, its email, calendar, and contacts functions) in the course of its business. Plaintiff Davenport also regularly uses Office 365's document functions.

34. The privacy and security of Plaintiff Davenport's and its clients' data are important and material to Plaintiff Davenport.

35. In deciding to subscribe to Office 365, Plaintiff Davenport believed Microsoft would keep Plaintiff Davenport's data private and secure.

36. Microsoft misrepresented and did not disclose to Plaintiff Davenport material facts, alleged more specifically below, regarding its use and protection of Plaintiff Davenport's data, and, as a result, Plaintiff Davenport was deceived. Had Microsoft not made these misrepresentations and had it properly disclosed these facts, Plaintiff Davenport would not have purchased its subscription, or alternatively would have paid less for it.

37. Since learning about Microsoft's improper sharing and use of business customer data, Plaintiff Davenport has ceased recommending that its clients purchase Office 365.

38. Plaintiff Davenport is investigating replacing its Microsoft subscription with a different solution, a transition that would require significant time and money.

JURISDICTION AND VENUE

39. The Court has subject matter jurisdiction under the Class Action Fairness Act, codified at 28 U.S.C. § 1332(d)(2). The matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, and is a class action in which any member of the class is a citizen of a State different from the Defendant.

40. Further, this matter also arises under the Wiretap Act, 18 U.S.C. § 2511, and the Stored Communications Act, 18 U.S.C. § 2702. The dispute is thus premised on a federal question, for which jurisdiction resides in this Court under 28 U.S.C. § 1331.

41. Insofar as Plaintiffs assert claims arising under state law, supplemental jurisdiction lies in this Court under 28 U.S.C. § 1367(a), as those claims are so related to Plaintiffs' federal claims that they form part of the same case or controversy.

42. In addition, Plaintiffs' claims arose and were caused by Microsoft's actions in California. Microsoft's misrepresentations to Plaintiffs and other actions took place in California, were aimed at Plaintiffs in California, and injured Plaintiffs in California. Microsoft knew its actions could reasonably and fairly subject it to suit and specific jurisdiction in California.

43. Microsoft's acts and omissions giving rise to Plaintiffs' claims were directed at Plaintiffs Russo and Koonan at their respective headquarters in Napa and San Francisco, in the

Northern District of California. This District is therefore a proper venue for this action, as prescribed by 28 U.S.C. § 1391.

FACTS

A. MICROSOFT TRANSITIONED BUSINESS CUSTOMERS TO ITS CLOUD-BASED SERVICES, ASSURING THEM THEIR DATA WOULD BE PRIVATE AND SECURE.

44. As the largest software company in the world, Microsoft led the transition to cloud computing.

45. Building on the enormous success of its Office suite of software products (including Word, Outlook, Excel, and PowerPoint), Microsoft developed Office 365 as a cloud-based "software-as-a-service" version of those popular offerings, for which customers would pay a monthly subscription fee.

46. "Trust" has been—and is—the centerpiece of Microsoft's advertising campaigns for its cloud-based business services and products. In its website "Trust Center," Microsoft promises it abides by the most "stringent privacy standards" and provides FAQs, videos, top-10 lists, and whitepapers declaring fidelity to customers' privacy demands.

47. Microsoft has focused on "trust" because it recognizes that "[o]ur business can succeed only if our customers trust us to protect their privacy and use their data in the ways that they permit us." Exhibit 1. As Microsoft Corporate Vice President and Deputy General Counsel Rich Sauer put it, Microsoft's corporate mission "depends on our ability to win and retain our users' trust." Exhibit 2 at 11. And internal Microsoft documents recognize that business customers will not use Microsoft's online services and products if they lack strong privacy protections.

48. Microsoft touts security, privacy, compliance, and transparency as the "foundational principles" of its "Trusted Cloud":

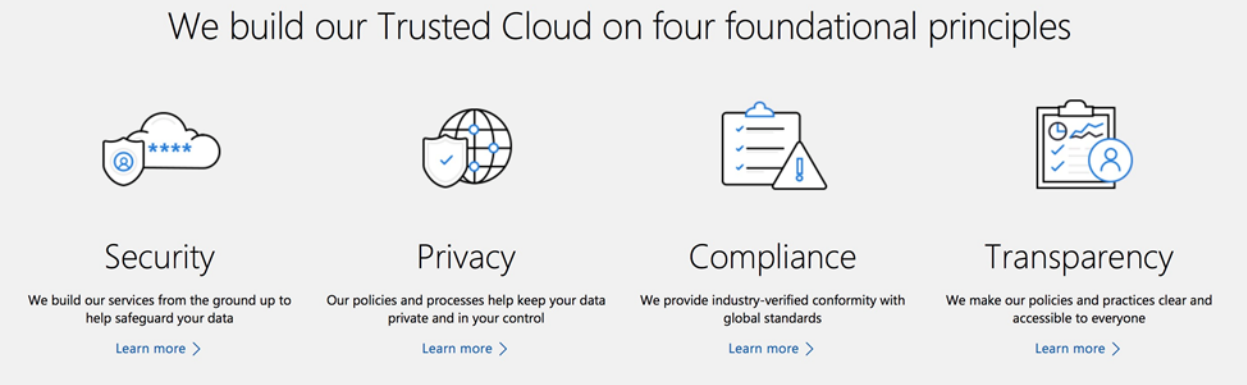


Exhibit 3.

49. Microsoft's marketing focus on privacy and security is also calculated to increase its bottom line. In internal documents, Microsoft identified privacy as a "competitive differentiator," noting that "[l]oyalty goes up with choice and control."

50. Microsoft knew that its customers were concerned about the security of storing information outside of their own networks or in a cloud infrastructure. As Microsoft put it, "[C]ustomers of all kinds have the same basic concerns about moving to the cloud. They want to retain control of their data, and they want that data to be kept secure and private[.]" Exhibit 4 at 5.

51. A business's data is among the most valuable assets it owns. Business data typically includes sensitive information, such as confidential financial details, secret business ideas, plans for new products or services, trade secrets, and other proprietary business insights and intelligence.

52. Business data can also include personal information about the businesses' customers and employees, including banking information, social security numbers, and other legally protected personally identifying information.

53. Businesses must protect their data, and they will pay more for that protection.

B. MICROSOFT'S PRIVACY AND SECURITY REPRESENTATIONS.

54. In its agreements and marketing materials directed to its business customers, Microsoft consistently represented that it would use their data only to provide them with the specific services they purchased.

55. Microsoft's agreements with its business customers define "customer data" as "all data, including all text, sound, software, image or video files that are provided to Microsoft by, or on behalf of, Customer" through the use of Office 365 or Exchange Online. Exhibit 5 at 5; Exhibit 6 at 1; *see also* Exhibit 7.

56. "Customer data" includes the customer's "content," *i.e.*, what Microsoft customers create, communicate, and store on or through Microsoft's services, such as the words in an email exchanged between friends or business colleagues, and the photographs and documents stored on Office 365 or Exchange Online. Exhibits 8, 9, 10.

57. Customer data also includes Exchange Online emails and attachments, Power BI (business intelligence) reports, SharePoint Online site content, and instant message ("IM") conversations. Exhibit 11.

58. Throughout its Trust Center, and in its related marketing materials, whitepapers, technical instructions, and other representations and documents, Microsoft has consistently represented to its business customers that their data will not be used for any purpose other than providing the specific services the customer has purchased. For example:

a. On a marketing page of its website, Microsoft promises, "We use your data for just what you pay us for: to maintain and provide Office 365[.] We make it our policy to not use your data for other purposes." Exhibit 7.

b. Similarly, in a whitepaper, Microsoft says that it "uses customer data only for providing cloud services. . . . We also don't scan our customers' email or documents for building analytics, data mining, advertising, or improving services without our customers' permission." Exhibit 12 at 7.

c. And in webpages designed to provide more technical information, Microsoft promises: "We use customer data only to provide the services; therefore, Microsoft strictly prohibits access to customer data for any other purpose." Exhibit 10.

59. Microsoft has also repeatedly guaranteed its business customers that they—and they alone—have control of their data. The Trust Center screenshot below is typical of the tone, tenor, and content of Microsoft's efforts and promises in this regard:

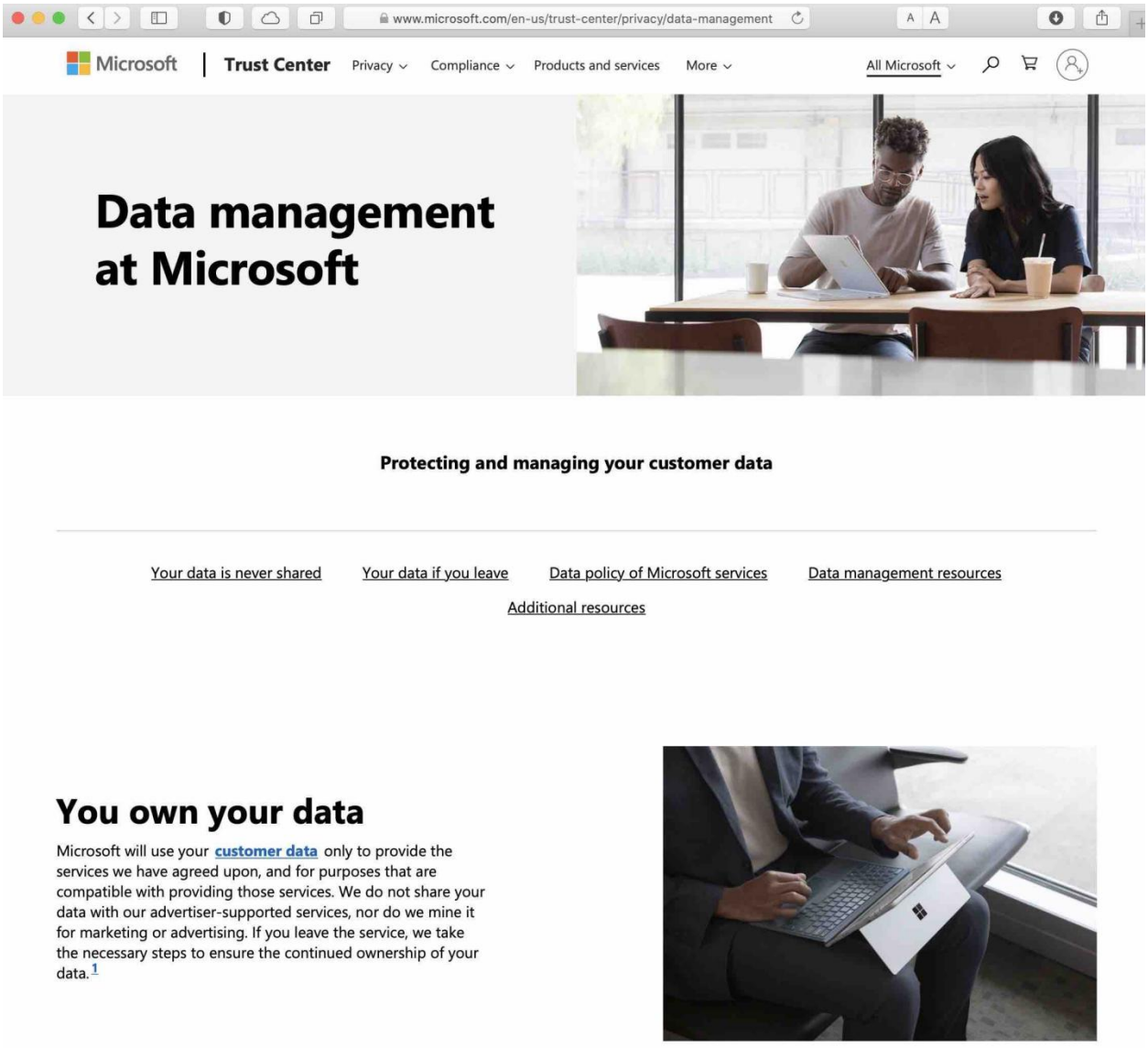


Exhibit 13.

60. This representation has remained consistent throughout the class period. For example, prior versions of Microsoft's webpages similarly promised:

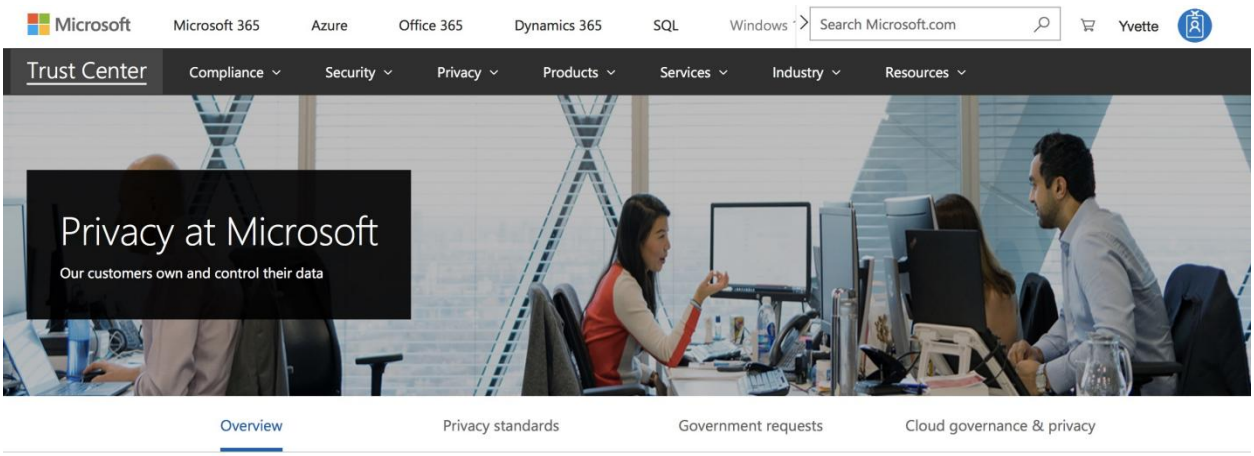


Exhibit 14.

61. These guarantees have been repeated to Microsoft's business customers in myriad materials. For example:

a. "As a customer of Office 365, you own and control your data. We do not use your data for anything other than providing you with the service that you have subscribed for. . . . You own your data and retain all rights, title, and interest in the data you store with Office 365." Exhibit 15.

b. "Our cloud services allow you to control who has access to your data, and how it's shared. . . . And you can take your data with you when you leave." Exhibit 16.

62. To that end, Microsoft has promised its customers that they can easily learn who has access to their data, and that they can terminate that access if they wish. For example:

a. "We are transparent about our privacy practices and offer meaningful privacy choices." Exhibit 16.

b. "We will be transparent about data collection and use so you can make informed decisions. . . . Also, you can take your data with you if you end your subscription." Exhibit 12 at 3, 8.

c. "With Office 365, it's your data. You own it. You control it. And it is yours to take with you if you decide to leave the service. . . . You know where your data resides and who has access[.]" Exhibit 17.

d. "We provide you with clear explanations about . . . who can access [your data] and under what circumstances." Exhibit 18 at 3.

63. Microsoft has also regularly represented that it "will not transfer to any third party (not even for storage purposes) data that you provide to Microsoft through the use of our business cloud services that are covered under the Microsoft Online Services Terms." Exhibit 19 at 3.

64. Microsoft has made—and continues to make—these and similar representations in many other marketing materials, too numerous and voluminous to list.

65. Microsoft has also made—and continues to make—these representations in its Online Service Terms, which apply to all business customers. In the Online Service Terms, and more specifically its 2020 Data Protection Agreement ("DPA"), Microsoft promised all business customers in the putative class that it would use their data "only (a) to provide Customer the Online Services in accordance with Customer's documented instructions, and (b) for Microsoft's legitimate business operations, each as detailed and limited below." The DPA clarifies that the customer, not Microsoft, "retains all right, title and interest in and to Customer Data," and narrowly defines the provision of online service as "[d]elivering functional capabilities" of the product purchased, troubleshooting problems, and improving the product through updates to improve "user productivity, reliability, efficacy, and security."

66. And the DPA specifies that Microsoft will not use business customer data for a broad range of activities unrelated to providing the purchased product, including "(a) user profiling, (b) advertising or similar commercial purposes, or (c) market research aimed at

creating new functionalities, services, or products or any other purpose, unless such use or processing is in accordance with Customer's documented instructions." Exhibit 20 at 5.

67. Though Microsoft amends the Online Service Terms from time to time, they have not materially changed vis-à-vis the putative class members and their claims during the class period.

68. For example, in the 2015 Online Service Terms, Microsoft promised its business customers:

> Customer Data will be used only to provide Customer the Online Services including purposes compatible with providing those services. Microsoft will not use Customer Data or derive information from it for any advertising or similar commercial purposes. . . . Microsoft will not disclose Customer Data or Support Data outside of Microsoft or its controlled subsidiaries and affiliates except (1) as Customer directs, (2) as described in the [Online Service Terms], or (3) as required by law.

Exhibits 21 at 7, 22 at 7.

69. Microsoft further "agrees and warrants . . . to process the personal data only on behalf of" the Microsoft business customer. Exhibits 21 at 27, 22 at 31.

70. Microsoft commits, moreover, that it "shall not subcontract any of its processing operations performed on behalf of" the Microsoft business customer without the customer's prior written consent. Exhibits 21 at 29, 22 at 33.

71. Microsoft's subscription and licensing agreements with class members reinforce these representations. For example, Microsoft's Business and Services Agreement says it will use business customer data "only for purposes of the parties' business relationship. [Microsoft will not] disclose [customer data] to third parties, except to its employees, Affiliates, contractors, advisors, and consultants ('Representatives') and then only on a need-to-know basis[.]" Exhibit 6 at 3.

72. Similarly, Microsoft's Open Value Agreement states that it will use business customer data "only for purposes of the parties' business relationship under this Agreement. [Microsoft will not] disclose that information to third parties, except to its employees, Affiliates,

resellers, contractors, advisors, and consultants (collectively, 'Representatives') and then only on a need-to-know basis[.]" Exhibit 5 at 10.

73. Reaffirming that message, Microsoft's Cloud Agreement and Open License Agreement say that the customer consents only "to the processing of personal information by Microsoft and its agents to facilitate the subject matter of this agreement." Exhibits 23 at §4b, 24 at §11, 25 at §11.

74. As alleged *infra* ¶¶ 129-132, Microsoft also promises business customers that it complies with SOC 1 and SOC 2 standards. Microsoft makes this representation for all products at issue in this action – including Office 365 and Exchange Online. Exhibits 26, 27.

C. MICROSOFT'S REPRESENTATIONS WERE FALSE.

75. ***Sharing.*** Microsoft promised its business customers that it would not ***share*** their data with others unless needed to perform the purchased services. Yet Microsoft in fact shared all business customers' Outlook contact data—which necessarily includes Plaintiffs'—with Facebook without consent, even if the customer was not a Facebook user, even if their contacts were not Facebook users. Microsoft also shared all business customers' data with subcontractors so Microsoft could develop new products and services. *See infra*.

76. ***Using.*** Microsoft promised its business customers that it would not ***use*** their data except to provide the services. Yet Microsoft in fact used all business customers' data, including communications like emails, to create new products it sold others, such as Security Graph API and Audience Network. *See infra*. Microsoft also exposed all business customers' data in a data-capturing program called "Graph" that allowed third parties to see and use non-consenting business customers' data. *See infra.*

77. ***Failing to Secure***. Microsoft promised its business customers that their data was secured using SOC 1 and SOC 2 compliant standards. Yet Microsoft in fact did not secure their data as promised, and instead exposed all business customers' data in the Graph data capturing program, which is neither SOC 1 nor SOC 2 compliant. *See infra*.

78. Each aspect of Microsoft's broken promises—sharing, using, and failing to secure—are discussed more fully below.

1. Sharing: Microsoft falsely promises it will not disclose business customers' data to third parties except as needed to provide the services and only with the business customers' consent.

79. As alleged *supra*, Microsoft regularly represented that it will not disclose businesses' Customer Data—which necessarily includes Plaintiffs'—to third parties except on a need-to-know basis. *See* ¶¶ 71-72, *supra*. (Microsoft "will not transfer to any third party (not even for storage purposes) data that you provide to Microsoft through the use of our business cloud services[.]"; Microsoft will not "disclose that information to third parties . . . and then only on a need-to-know basis").

80. As alleged *supra*, Microsoft also regularly represented that it will not disclose businesses' Customer Data to third parties unless the business customer consents. *See* ¶¶ 68, 70-71, *supra*. (Microsoft "shall not subcontract any of its processing operations" without the customer's consent; "Microsoft will not disclose Customer Data or Support Data outside of Microsoft . . . except (1) as Customer directs[.]").

81. Microsoft's representations are false. Without their consent, and without a need to know, Microsoft shares businesses' Customer Data with Facebook and other third parties, as specified below.

a. Facebook

82. Facebook is the world's largest social media network, with over two billion active users. Its business model relies on using and sharing its users' data.

83. Although Facebook is not necessary to provide Office 365 or Exchange Online services to Microsoft's business customers, Microsoft routinely and automatically shares its business customers' contacts—including Plaintiffs'—with Facebook—without those customers' consent—whether or not the customers or their contacts are Facebook users.

84. Even if a customer discovers and disables Facebook sharing after activating Office 365 or Exchange Online services, the damage has already been done. At that point, the business customer's contacts have been shared with Facebook. As Microsoft explains in an obscure technical instruction, "[o]nce contacts are transferred to Facebook, they cannot be deleted from Facebook's systems except by Facebook." Exhibit 28 at 6.

85. No Plaintiff consented to Facebook sharing, and no Plaintiff was aware that their contact information was automatically shared with Facebook in the manner described above.

86. Each Plaintiff's Outlook contact data was transferred to Facebook without their consent.

87. Because Microsoft shares its business customers' contact data with Facebook, its customers' data is accessible not just by Facebook, but also by whomever Facebook shares the data with, and whomever *those* entities decide to share the data with, *ad infinitum.*

88. For example, after Facebook gave limited data access to University of Cambridge psychology lecturer Aleksandr Kogan, data of 87 million persons were exploited by Cambridge Analytica, a data mining firm that focuses on opposition research and intelligence gathering for political campaigns.

89. With Facebook's data, Cambridge Analytica was able to create a political microtargeting platform that identified which issues mattered to the voter and, with eerie precision, use machine learning and sentiment manipulation to influence them to vote (or not vote).

90. Cybercriminals and hackers use Facebook data to tie an individual or company to datasets previously scrubbed of identifying information. By piecing together seemingly random data points, hackers and cybercriminals are able to sell sensitive commercial information in the black market or the dark web, from login passwords to inside information that make for profitable stock trades.

b. Subcontractors

91. Contrary to its promise to not share business customers' data with third parties unless needed to perform the services and only with the business customers' consent, Microsoft uses and shares business customers' data—including the content of their documents, emails, email attachments, text, audio, and video files—with hundreds of subcontractors (or "subprocessors," as Microsoft sometimes calls them), not only to provide customers with the services they purchased, but also to serve Microsoft's separate commercial ventures, including

discovering new business insights and developing new services, products, or features for Microsoft's benefit, such as artificial intelligence applications and development interfaces.

92. In fact, Microsoft's written "Supplier Data Protection Requirements" explicitly permit suppliers to use customers' personal data in a development environment. Exhibit 29 at 19, ¶ 76.

93. Before using business customers' information in development, Microsoft asks that the developer anonymize only a minuscule portion of customers' data, *e.g.*, social security numbers, and does not disclose that fact to its business customers. Exhibit 29 at 1, 19 ¶ 76.

94. Microsoft does not require its subcontractors to encrypt business customers' data and does not disclose that fact to its business customers. Rather, Microsoft requires these subcontractors to encrypt only a limited subset of the data (and only when at rest)—usernames and passwords, credit card and bank account numbers, medical record numbers or biometric identifiers, and government-issued identification data. Exhibit 29 at 18, ¶ 72.

95. Microsoft's sharing of its business customers' data with its subcontractors creates a security and privacy risk, is not disclosed, and is contrary to the representations Microsoft makes to its business customers regarding data privacy and security.

96. Microsoft shared all Plaintiffs' and its business customers' customer data with subcontractors though it was not necessary to provide Plaintiffs with their purchased products.

c. Other third parties

97. Contrary to its promise to not share customer data except on a need-to-know basis with customers' consent, Microsoft shares Plaintiffs' and its business customers' data with countless others.

98. As just one example, Microsoft gathers all users' availability status (such as "Available" or "Away"), a color-coded presence indicator, users' schedules, locations, and personal or out-of-office notes. By default (and without users' express consent), Microsoft shares this "Lync Presence" data with "anyone who can communicate" with that user – even if they are not in the user's contacts. Microsoft does not permit users to keep their Lync Presence data

private. At most, users can limit their Lync Presence data to be shared only with those in their contacts. Exhibit 28 at 29-31.

2. Using: Microsoft falsely promises it will use business customers' data only as needed to provide the services, but in fact uses it to develop and sell new products and services for Microsoft's own benefit.

99. As alleged *supra*, Microsoft regularly represented that it will not use businesses' Customer Data except to provide the services the customer purchased. *See* ¶¶ 58-61, 65-66, 68-69, 71-72, *supra*. ("Microsoft will not use Customer Data or derive information from it for any advertising or similar commercial purposes[.]").

100. Microsoft's representation is false. Contrary to its disclosures to and agreements with its business customers, Microsoft uses all Plaintiffs' and all business customers' data for its own commercial purposes, including to develop and sell new products and services to others. *See generally* Exhibit 30 (Keynote Address by Satya Nadella, Microsoft CEO).

a. Microsoft uses business customers' email and account data to create Security Graph API, which it sells to others.

101. Microsoft harvests business customer data to develop and sell other products, including Security Graph API, an application program interface Microsoft sells to software developers so they can create new security-related products. Exhibits 31, 32.

102. Microsoft boasts that Security Graph API is built off the "uniquely broad and deep" insights Microsoft obtained for itself by scanning "400 billion" of its customers' emails and "data from 700 million Azure user accounts." Exhibit 31 at 6, 7, 9.

b. Microsoft collects all business customers' data into a data capturing program called Graph, which it uses to create additional products it sells to others.

103. Microsoft collects all its business customers' data (including all emails, documents, calendar entries, addressbook data, etc.) into a data-capturing program called "Graph." Like it does for all business customers, Microsoft collected all the Plaintiffs' data into Graph.

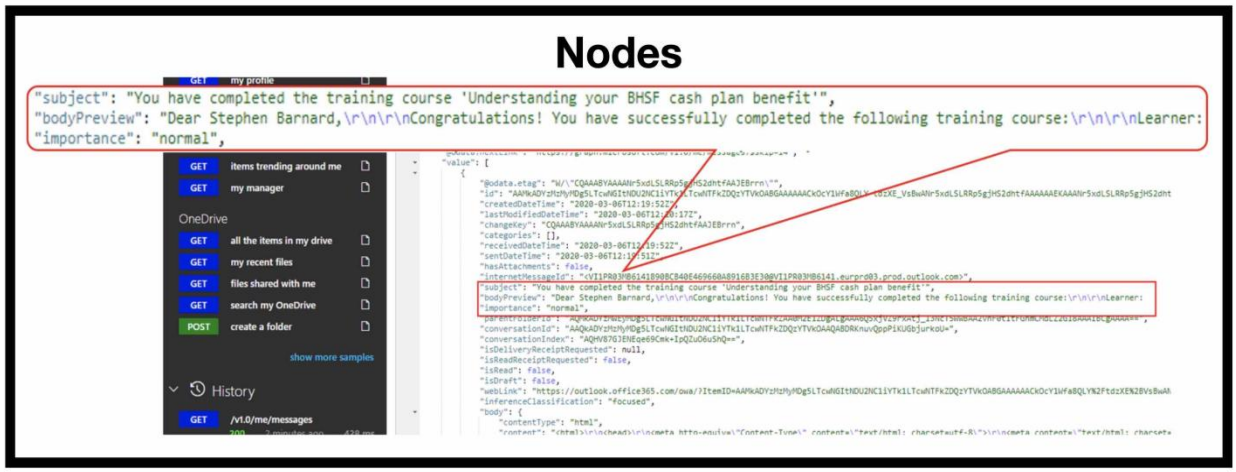
104. Microsoft mines this Graph data so that it can develop new products that it sells to other customers.

105. Microsoft Graph collects all data across the business cloud platform. Exhibit 33 at 1. As Microsoft recognizes, Graph collects "the things they care about most: their mail, calendars, contacts, users and groups, files, and folders." Exhibit 34 at 1.

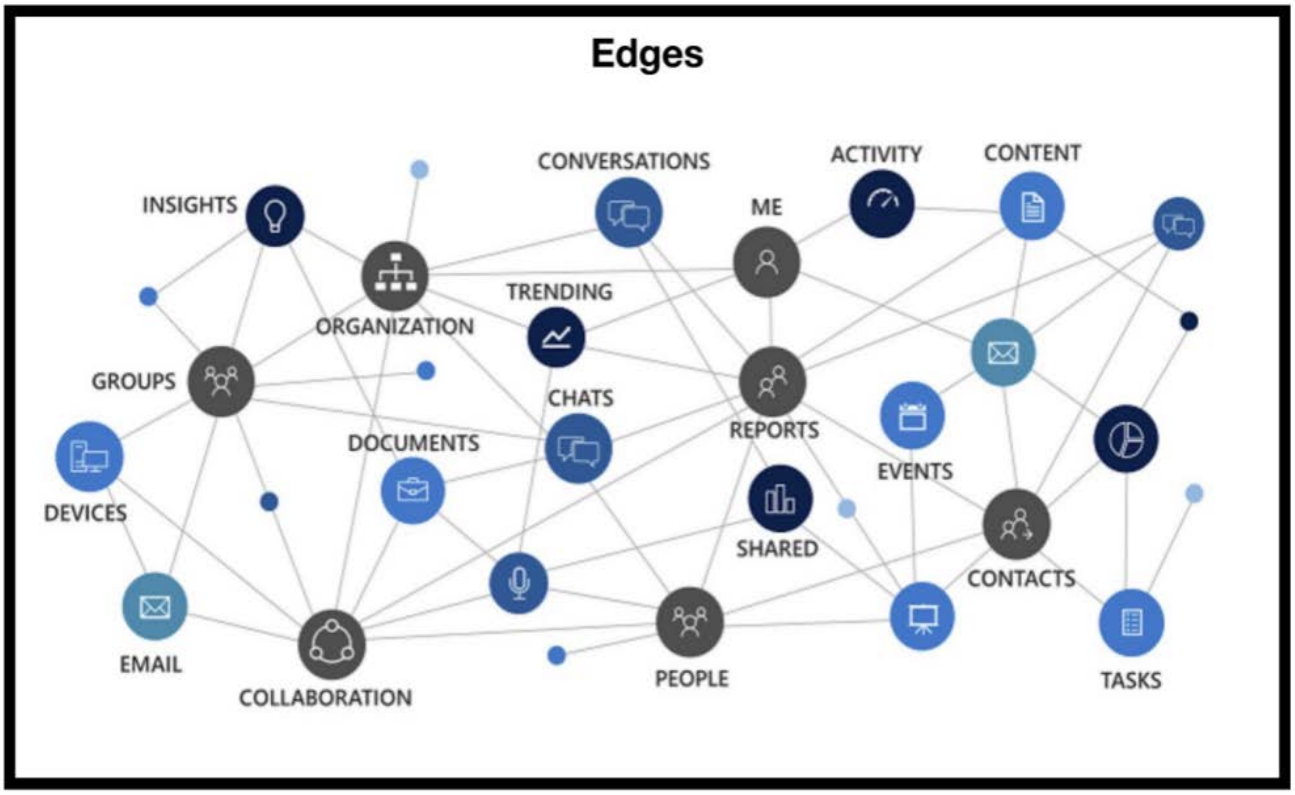
106. Graph collects two types of business customers' Office 365 data: (1) "nodes," or metadata points, such as an email's content, subject, and sender, and (2) "edges," which describe the relationship between the data, *e.g.*, that a person sent an email is in the user's contacts, or other documents sent by that user. Exhibit 35,

107. The "nodes" in Microsoft Graph expose an enormous amount of Office 365 data. For emails, Graph will identify the content of the email body, its subject, to whom it was sent, when, what documents were attached, and more. Exhibit 36. For Outlook contacts data, Graph's nodes will identify and capture the name, profession, whether it is a "favorite," the contact's notes, and similar data. Exhibits 37, 38. For Outlook events, Graph's nodes will capture the event's title, attendees, location, and sensitivity ("normal," "personal," "private," "confidential"), among other information. Exhibit 39. Graph also collects business customers' data for other key Microsoft services, like tasks, documents, and more, Exhibit 40.

108. As "nodes," Microsoft Graph keeps discrete pieces of information about every email, notes, events, contacts, documents, and other Office 365 item. The below image, obtained from https://www.poweronplatforms.com/using-microsoft-graph-explorer/, shows an example of the information captured by Microsoft Graph for an email. To illustrate, Microsoft captures in Graph the date an email was created as "createdDateTime." (See third line in the image below.) Microsoft Graph captures the email's subject, body, and "importance." (See the callout of the middle lines and the last line in the image below.) Other lines show whether a document was attached to the email, when it was sent, when it was received, whether it was read, the email's recipients, persons copied on the email, and persons "blind" copied on the email. Exhibit 36 at 10-11.



109. Microsoft Graph also analyzes the relationships between these nodes, capturing them in "edges." Exhibit 35. For example, for Outlook contacts, Graph aggregates information about a particular contact from across e-mail, social networks, Skype, and others.



110. Microsoft Graph collects and analyzes this data without consent. Graph analyzes this data for all business customers and does not wait until a business customer consented. It also does not wait until another person the business customer communicates with has consented.

111. Microsoft funnels all business customers' data into Graph, automatically and without their consent. It is turned on by default. Exhibit 28 at 28.

112. Microsoft uses business customers' data—including that of the Plaintiffs and class members—captured in Graph to sell new products to others.

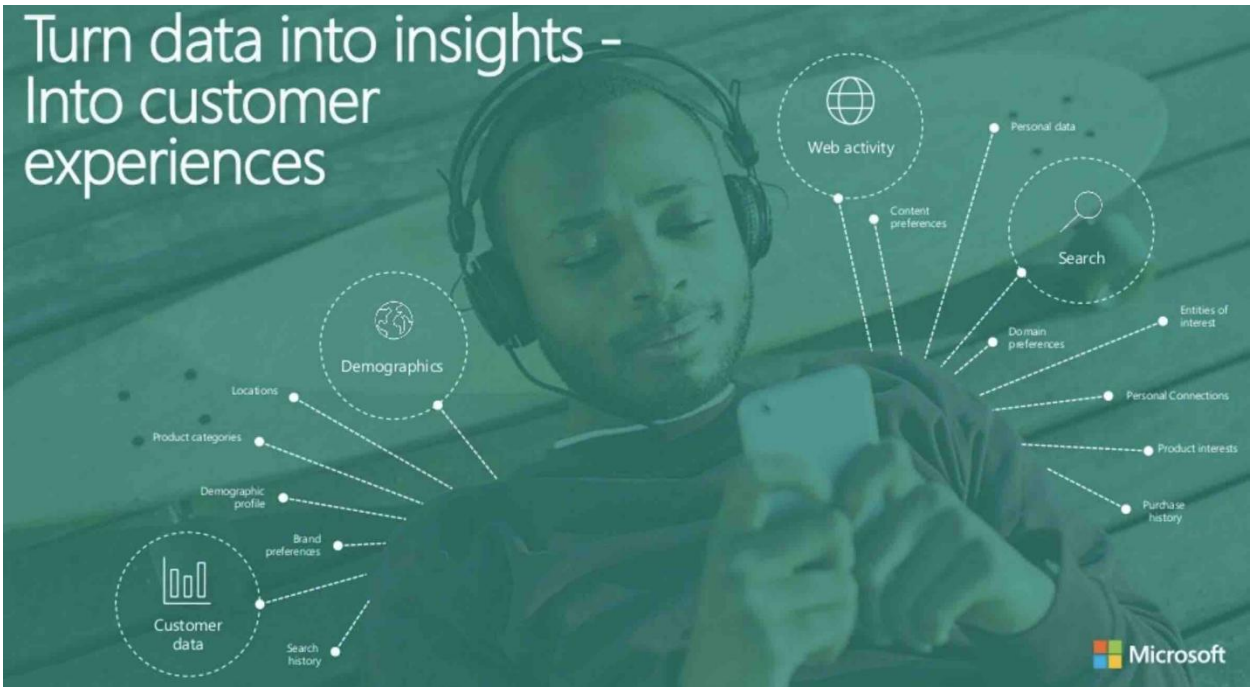
113. For example, Microsoft harvests Graph data to develop and sell to others a marketing product called Microsoft Audience Network, which Microsoft admits derives enormous value from processing customer data. In Microsoft's own words:

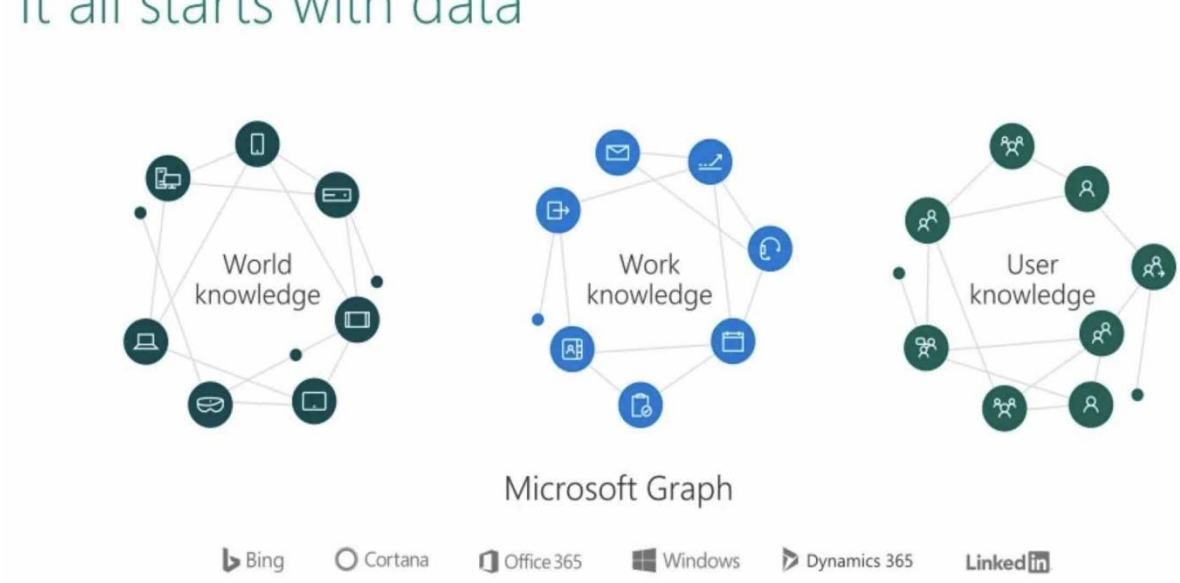
> What sets Microsoft Audience Ads apart is their rich user understanding that powers high performance. The Microsoft Graph consists of robust data sets, including search and web activity, LinkedIn professional profiles, demographics and more. The data is continually updated every second based on user activities. By mapping audience data on such an enormous scale, the Graph helps us spot trends and uncover insights, both of which allow you to effectively reach your customers.

Exhibit 41.

114. As Microsoft further explains regarding Microsoft Audience Network, it finds "new potential customers" by analyzing "search history, activity on Bing and other Microsoft properties, and user profile data." Exhibit 42 at 1.

115. As one Microsoft Search Advertising executive explained it, turning data into customer insights "all starts with data." Simon Jacobson, Keynote address at Digimarcon 2018, Artificial Intelligence or is it Intelligence Amplified, *available at* https://www.slideshare.net/digimarcon/artificial-intelligence-or-is-it-intelligence-amplified-simon-jacobson-microsoft.





116. Microsoft also shares Graph data with third-party developers, so they can develop and sell new services and products, at additional profit to Microsoft, either directly or indirectly.

117. Among other things, Microsoft gives third-party developers information about the documents and projects those non-consenting business customers worked on. Microsoft allows those third-party developers to scan and search the content of its business customers' emails and

to access their schedules, locations, and availability status, *i.e.*, whether they are "available" or "away." *See* Exhibits 37, 28 at 29.

118. In advertising its developer platform to third-party developers, Microsoft touts the enormous value of its customers' data, highlighting how developers will get data not just about the authorized user, but also about other users who communicate with the authorized user. Exhibits 43, 44.

119. As Microsoft explains: "Microsoft Graph is the gateway to data and intelligence in Microsoft 365 . . . that you can use to take advantage of the tremendous amount of data in Office 365[.]" Exhibit 43 at 1.

120. For example, Microsoft explains to developers that they can "perform searches for people who are relevant to the [Microsoft] user and have expressed an interest in communicating with that user" about specific topics. Microsoft explains that "[t]opics in this context are just words that have been used most by users in email conversations. Microsoft extracts such words and creates an index for this data to facilitate . . . searches." Exhibit 37 at 17.

121. Microsoft does not require those third-party developers to employ the security measures that Microsoft has promised its business customers. Instead, Microsoft only requests that they employ "reasonable security measures." Exhibit 45 at 8. The actual level of security used by those third-party developers is unknown and not reasonably knowable to Plaintiffs.

122. Microsoft profits from sharing its business customers' Office 365 data by charging the developers directly for access, accepting a commission from sales of the products developed from its customers' data, or other means.

123. These separate products it sells to others, including the Security Graph, Microsoft Audience Network, and Microsoft's third-party developer platform, are not necessary to provide Office 365 services.

124. In sum, despite its promises to use business customers' data only for the purpose of providing the customers with the purchased services, Microsoft uses the data for its own purposes: to create and sell new products to others.

3. Failing to Secure: Microsoft falsely promises it protects business customers' data using SOC-compliant standards, but in fact does not.

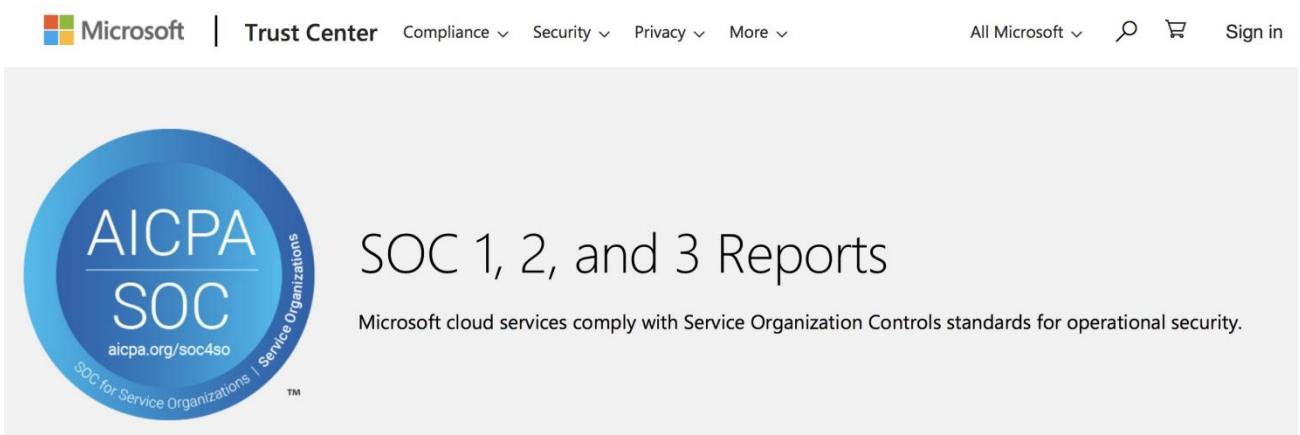
125. Microsoft not only misleads its business customers as to how it shares and uses their data, but also misleads them regarding how it protects and processes that data.

126. Microsoft knows that business customers would not share their data with a service provider whose security that did not comply with "System and Organization Controls" or "SOC" standards.

127. "SOC" is the standard adopted by the American Institute of Certified Public Accountants for controls that safeguard the confidentiality and privacy of information stored and processed in the cloud. Exhibits 26, 27.

128. Microsoft also knows that many business customers must satisfy SOC compliance for their own business operations. For example, businesses performing services for governmental or quasi-governmental entities must satisfy SOC compliance requirements.

129. Microsoft promises business customers that it complies with SOC 1 and SOC 2 standards. For example, in Microsoft's "Trust Center," Microsoft states:



Exhibits 26; *see also* Exhibit 27.

130. Microsoft represents in addition:

> Microsoft cloud services comply with Service Organization Controls standards for operational security.
>
> . . . .

> Microsoft covered cloud services are audited at least annually against the SOC reporting framework by independent third-party auditors. The audit for Microsoft cloud services covers controls for data security, availability, processing integrity, and confidentiality as applicable to in-scope trust principles for each service.
>
> Microsoft has achieved SOC 1 Type 2, SOC 2 Type 2, and SOC 3 reports.

Exhibit 26 at 1.

131. Microsoft makes this representation for all products at issue in this action – including Office 365 and Exchange Online. Exhibits 26, 27, 46.

132. Microsoft encourages its customers to rely on its promises of SOC compliance. For example, as Microsoft explains through one of its marketing materials:

> Q. Can I leverage Microsoft's compliance in my organization's certification process?
>
> Yes. When you migrate your applications and data to Microsoft's covered cloud services, you can build on the audits and certifications that Microsoft holds. The independent reports attest to the effectiveness of controls Microsoft has implemented to help maintain the security and privacy of your data.

Exhibit 27 at 2; *see also* Exhibit 46.

133. These promises are false.

134. By default, automatically and without its customers' knowledge or consent, Microsoft collects its business customers' data – including emails of each Plaintiff and all class members – into its data collection program, Graph. *See supra* at ¶¶ 103-111.

135. As Microsoft admits in its own documentation, Graph complies with neither SOC-1 nor SOC-2 standards:

Online Service	ISO 27001	ISO 27002 Code of Practice	ISO 27018 Code of Practice	SSAE 16 SOC 1 Type II	SSAE 16 SOC 2 Type II
Microsoft Graph	Yes	Yes	Yes	No	No

Exhibit 22 at 13.

136. Because Microsoft's Graph automatically gathers all business customers' Office 365 and Exchange Online data, *see supra* at ¶¶ 103-111, and Graph does not comply with SOC standards, Microsoft's handling and use of business customers' Office 365 and Exchange Online data also does not comply with SOC standards.

D. MICROSOFT'S ACTIONS HAVE INJURED PLAINTIFFS AND OTHER BUSINESS CUSTOMERS.

137. Plaintiffs did not receive the Microsoft products and services they were promised.

138. Plaintiffs and Microsoft's other business customers would not have purchased (or would have paid less for) Microsoft's services if Microsoft had not made the misrepresentations discussed above and had disclosed its sharing and use of its customers' data.

139. Microsoft's use and sharing of Plaintiffs' and Microsoft's other business customers' data also reduced their data's privacy and security.

CLASS ACTION ALLEGATIONS

140. Plaintiffs make these allegations on their own behalf, and on behalf of a class of similarly situated Microsoft business customers ("Class Members"), defined as:

> All persons and non-governmental entities in the United States who subscribed to or purchased Microsoft Office 365 Business, Microsoft Office 365 Business Essentials, Microsoft Office 365 Business Premium, Exchange Online Plan 1, Exchange Online Plan 2, Microsoft Office 365 Enterprise, Office 365 Enterprise, Microsoft 365 Enterprise, Microsoft 365 Business, Office 365 Business, Office 365 Pro Plus, Office 365 Business Essentials, Office 365 Business Premium, Microsoft 365 Business Basic, Microsoft 365 Business Standard, or Microsoft 365 Business Premium, but did not subscribe to or purchase Microsoft Cognitive Services, from July 17, 2016, through the present (the "Class Period").

141. Excluded from the Class are governmental entities, Microsoft and any entity in which Microsoft has a controlling interest, Microsoft's employees, any Judge to whom this action is assigned, any member of the Judge's staff or immediate family, and counsel for any party.

142. Plaintiffs reserve the right to alter their proposed class definition as warranted by the evidence obtained through discovery.

143. Class Members are readily ascertainable based on Microsoft's own records.

144. The proposed class meets all certification requirements of Federal Rules of Civil Procedure 23(a) and 23(b)(3).

145. Because there are millions of Class Members, the Class is sufficiently numerous.

146. There are many questions of law or fact common to Plaintiffs and Class Members, including:

a. Whether Microsoft engaged in false, deceptive, or misleading business practices;

b. Whether Microsoft used the Class Members' data for its own unauthorized, commercial purposes;

c. Whether Microsoft shared the Class Members' data with unauthorized third parties;

d. Whether the Class Members consented to Microsoft's sharing and use of their data;

e. Whether the Class Members are entitled to statutory damages for Microsoft's actions;

f. Whether Microsoft's conduct violated the statutes as alleged below;

g. Whether the Class Members are entitled to compensatory damages for Microsoft's actions;

h. Whether the Class Members are entitled to punitive damages for Microsoft's actions; and

i. Whether the Class Members are entitled to declaratory and injunctive relief for Microsoft's actions.

147. Plaintiffs' claims are typical of the claims of Class Members. Plaintiffs have suffered the same injuries as other Class Members, and their interests are aligned with the interests of the other Class Members.

148. Plaintiffs subscribed to or purchased substantially the same services or products as all Class Members; Microsoft made the same material misrepresentations and omissions to each Class Member; these misrepresentations were false and omissions were wrongful for the

same reasons; each Class Member's data was wrongfully used and shared, and Microsoft otherwise violated Plaintiffs' and the Class Members' rights in the same way.

149. Plaintiffs are adequate representatives of the Class with no conflicts of interest who have obtained capable and experienced counsel to prosecute the Class Members' claims.

150. Questions and issues common to the Class will predominate over any individualized inquiries.

151. A class action is superior to individual cases, especially because the costs of litigating individual Class Members' claims would far surpass their individual recoveries.

APPLICABLE LAW

152. The federal claims in this case are based on the statutes cited in Counts One and Two below.

153. The state law claims are based on Washington statutory and common law because Microsoft has chosen the nationwide application of Washington law to its business customers.

154. For example, Microsoft's Open Value Agreement provides: "Applicable law. The terms of this agreement entered into with any Microsoft Affiliate located outside of Europe will be governed by and construed in accordance with the laws of the State of Washington and federal laws of the United States."

155. Similarly, Microsoft's Business and Services Agreement provides as follows: "Applicable law**.** The terms of this agreement and/or any Supplemental Agreement entered into with any Microsoft Affiliate located outside of Europe will be governed by and construed in accordance with the laws of the State of Washington and federal laws of the United States."

156. Microsoft's other subscription and license agreements for business customers also state that its terms are to be governed by federal law and Washington state law.

157. State choice of law principles also make the application of Washington state law appropriate in this case.

Count One
Violations of the Wiretap Act
18 U.S.C. §§ 2511(1)(a), (1)(c), and (1)(d)
On behalf of Plaintiffs and the Class

158. The Wiretap Act, 18 U.S.C. § 2520, provides for damages and other relief against any person who:

a. intentionally intercepts or endeavors to intercept the contents of any electronic communication, *id.* § 2511(1)(a).

b. intentionally discloses or endeavors to disclose to any other person the contents of any electronic communication, knowing or having reason to know that the information was obtained through the interception of an electronic communication, *id.* § 2511(1)(c); or

c. intentionally uses or endeavors to use the contents of any electronic communication, knowing or having reason to know that the information was obtained through the interception of an electronic communication, *id.* § 2511(1)(d).

159. Business customer data transferred to Microsoft at the time of transmission through the customer's use of Office 365 or Exchange Online is an "electronic communication," which is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." *Id.* § 2510(12).

160. Plaintiffs used Microsoft's cloud services to send and receive communications, including sending and receiving emails through Microsoft's Outlook.

161. Plaintiffs and Class Members are "persons" under the Wiretap Act because they are an "individual, partnership, association, joint stock company, trust, or corporation." *Id.* § 2510(6).

162. Plaintiffs and Class Members are "users" under the Wiretap Act because they use Office 365 or Exchange Online, each of which is "an electronic communication service," and they are "duly authorized by [Microsoft] to engage in such use." *Id.* § 2510(13).

163. Plaintiffs and Class Members are "aggrieved persons" under the Wiretap Act because they are "a person who was a party to any intercepted . . . electronic communication or a person against whom the interception was directed[,]" *id.* § 2510(11), and they assert violations of 18 U.S.C. §§ 2511(1)(a), (1)(c), and (1)(d) for Microsoft's unlawful interception, disclosure, and use of their electronic communications.

164. Microsoft is a "person" under 18 U.S.C. § 2510(6) because it is an "individual, partnership, association, joint stock company, trust, or corporation."

165. Microsoft's cloud infrastructure is a "device" because it "can be used to intercept [an] . . . electronic communication[.]" *Id.* § 2510(5).

166. As alleged more fully above, Microsoft unlawfully intercepted in transmission, disclosed, and used without consent the Plaintiffs' and Class Members' data in the following non-exhaustive ways:

a. Microsoft obtained the content of their communications and emails, including attached documents, contacts, calendars, location data, audio files, photographs, and video files;

b. Microsoft shared that data with unauthorized third parties, including software application developers and hundreds of subcontractors, who use the data for their own purposes, or for purposes that benefit Microsoft; and

c. Microsoft used the data to glean business intelligence and develop new products – such as Microsoft Graph, Security Graph API, and Audience Network – to sell to others, and to improve products regardless of whether the business customer uses the product, without consent.

167. Through its use and sharing of business customer data as alleged above, Microsoft has intentionally **intercepted** or endeavored to intercept the contents of Plaintiffs' and Class Members' electronic communications, without consent, in violation of 18 U.S.C. § 2511(1)(a).

168. Microsoft is not the intended recipient of the electronic communications and is not a party to those communications. For example, in the case of emails sent by Plaintiffs and

Class Members, the intended recipient was not Microsoft, but the person or entity to whom the email was addressed.

169. Microsoft's intentional interception of Plaintiffs' and Class Members' data is not necessary or incidental to and does not facilitate the transmission of Plaintiffs' and Class Members' data. It is not needed to provide Plaintiffs and Class Members the Microsoft services for which they subscribed.

170. Through its use and sharing of business customer data as alleged above, Microsoft has intentionally **disclosed** or endeavored to disclose to other persons the contents of Plaintiffs' and Class Members' electronic communications, knowing or having reason to know that the information was obtained through the interception of an electronic communication, without consent, in violation of 18 U.S.C. § 2511(1)(c).

171. Through its use and sharing of business customer data as alleged above, Microsoft has intentionally **used** or endeavored to use the contents of Plaintiffs' and Class Members' electronic communications, knowing or having reason to know that the information was obtained through the interception of an electronic communication, without consent, in violation of 18 U.S.C. § 2511(1)(d).

172. Plaintiffs bring this claim based upon all allegations in this Amended Complaint, except the Facebook allegations in Part C.1.a.

173. Under 18 U.S.C. § 2520(a), Plaintiffs and Class Members are entitled to:

a. injunctive and declaratory relief;

b. for each Plaintiff and Class Member, damages equal to the greater of $1,000 or the sum of the actual damages suffered by that plaintiff and any profits made by Microsoft as a result of the violation;

c. punitive damages;

d. litigation costs; and

e. reasonable attorney's fees.

Count Two
Violations of the Stored Communications Act
18 U.S.C. § 2702
On behalf of Plaintiffs and the Class

174. The Stored Communications Act, 18 U.S.C. § 2707, provides for damages and other relief against any person who:

a. knowingly divulges to others the contents of electronic communications while in Microsoft's electronic storage, *id.* § 2702(a)(1);

b. knowingly divulges to others the contents of electronic communications maintained on Microsoft's service on behalf of, and received by means of electronic transmission from, Plaintiffs and Class Members, *id.* § 2702(a)(2)(A); or

c. knowingly divulges to others the contents of electronic communications carried or maintained on Microsoft's service solely for the purpose of providing storage or computer processing services to Plaintiffs and Class Members, *id.* § 2702(a)(2)(B).

175. Plaintiffs assert claims under the Stored Communications Act in the alternative to the Wiretap Act claim, in the event the Court finds that Microsoft obtains Plaintiffs' and Class Members' data while they are in "storage" rather than in "transit."

176. Microsoft provides an "electronic communications service" because it "provides to users thereof the ability to send or receive wire or electronic communications." *Id.* § 2510(15).

177. Plaintiffs' and Class Members' electronic communications are in "electronic storage" because, incidental to their electronic transmission, they are kept in temporary, intermediate storage. *Id.* § 2510(17).

178. Microsoft provides "remote computing service[s]" because it provides to the public "computer storage or processing services by means of an electronic communications system." *Id.* § 2711(2).

179. As alleged more fully above, Microsoft violated the Stored Communications Act with respect to the Plaintiffs and Class Members in the following non-exhaustive ways:

a. Microsoft obtained the content of their communications and emails, including attached documents, contacts, calendars, location data, audio files, photographs, and video files, without consent;

b. Microsoft shared that data with unauthorized third parties, including software application developers and hundreds of subcontractors, who use the data for their own purposes, or for purposes that benefit Microsoft, without consent; and

c. Microsoft used the data to glean business intelligence and develop new products – such as Microsoft Graph, Security Graph API, and Audience Network – to sell to others, and to improve products such regardless of whether the business customer uses the product, without consent.

180. Microsoft accessed without authorization its cloud infrastructure, which is "a facility through which an electronic communication service is provided," and obtained access to Plaintiffs' and Class Members' electronic communications, in violation of 18 U.S.C. § 2701(a)(1).

181. Through its use and sharing of business customer data as alleged above, Microsoft knowingly divulged to other entities the contents of Plaintiffs' and Class Members' electronic communications while in electronic storage by Microsoft, in violation of 18 U.S.C. § 2702(a)(1).

182. Through its use and sharing of business customer data as alleged above, Microsoft (as a provider of remote computing services) knowingly divulged to other entities the contents of Plaintiffs' and Class Members' electronic communications carried or maintained on Microsoft's service, in violation of 18 U.S.C. § 2702(a)(2).

183. Under § 2702(a)(2)(A), Plaintiffs' and Class Members' electronic communications are maintained on Microsoft's servers on their behalf, as they are subscribers and customers of Microsoft's service. Microsoft receives their electronic communications by means of electronic transmission (or by means of computer processing of communications received by means of electronic transmission) from them.

184. Under § 2702(a)(2)(B), Plaintiffs' and Class Members' electronic communications are carried or maintained on Microsoft's service solely for the purpose of

providing storage or computer processing services to them, and Microsoft is not authorized to access the contents of their communications for purposes of providing any services other than storage or computer processing.

185. Plaintiffs bring this claim based upon all allegations in this Amended Complaint, except the Facebook allegations in Part C.1.a.

186. Under 18 U.S.C. § 2707(b) and § 2707(c), Plaintiffs and Class Members are entitled to:

a. injunctive and declaratory relief;

b. for each Plaintiff and Class Member, damages equal to the greater of $1,000 or the sum of the actual damages suffered by that plaintiff and any profits made by Microsoft as a result of the violation;

c. punitive damages;

d. litigation costs; and

e. reasonable attorney's fees.

Count Three
Violations of the Washington Consumer Protection Act
RCW 19.86, et seq.
On behalf of Plaintiffs and the Class

187. Washington's Consumer Protection Act ("CPA"), RCW 19.86, *et seq.*, prohibits unfair competition and unfair and deceptive acts or practices in trade or commerce in order to protect both consumers and businesses, and to foster fair and honest competition.

188. Microsoft is a "person" within the meaning of the CPA, particularly RCW 19.86.010(1), and it conducts "trade" and "commerce" within the meaning of RCW 19.86.010(2).

189. Each Plaintiff is a "person" within the meaning of the CPA, particularly RCW 19.86.010(1).

190. As set forth above, Microsoft represented to business customers that it would use business customers' data only to provide the services they purchased (see *supra* at ¶¶ 58-61, 65-66, 68-69, 71-72); that it would share their data with certain representatives only on a need-to-

know basis (see *supra* at ¶¶ 71-72); that it will never share the customers' data with third parties at all (see *supra* at ¶¶ 59 ("Your data is never shared"), 63, 71-72); and that security used for business customers' data complied with SOC standards (see *supra* at ¶¶ 129-132).

191. As alleged *supra* in ¶¶ 75-136, those representations were false.

192. As set forth above, Microsoft engaged in unfair and deceptive acts or practices by adopting patterns and practices of:

a. making representations, omissions, and solicitations that, considering their net impression and viewed as a whole, have the capacity to deceive the purchasing public regarding Microsoft's use and sharing of business customer data, and its compliance with SOC standards;

b. failing to disclose material facts regarding its use and sharing of business customer data and compliance with SOC standards;

c. diminishing the security and privacy of its customers' data through its use and sharing of that data and noncompliance with SOC standards;

d. diminishing the security and privacy of its customers' data through its failure to adopt and enforce adequate data security protections, including SOC standards, both on its own systems and in the systems of third parties and representatives with which Microsoft has shared or transferred business customer data; and

e. falsely holding itself out as transparent and deserving of its customers' trust.

193. Based on the conduct alleged above, and other conduct that will be revealed through discovery, Microsoft has engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of RCW 19.86.020.

194. Microsoft's conduct affects the public interest because, *inter alia*:

a. Microsoft injured thousands of persons who paid for or paid more for a service advertised as having certain qualities, when in fact the product did not have those qualities, and whose data was used and shared without consent; and

b. Microsoft's unfair or deceptive acts or practices were committed in the course of its business;

c. Microsoft aggressively advertises its cloud-based services to the public in general;

d. Microsoft actively solicits businesses to subscribe to its cloud-based services;

e. Microsoft occupies an unequal bargaining position with respect to the businesses to which it sells its cloud-based services;

f. Microsoft is the largest software company in the world, and has enormous resources and extraordinary sophistication regarding use and sharing of business customer data, yet has abused that position in order to exploit its customers' data, and has done so through deception, nondisclosure, and inadequate disclosure.

195. Plaintiffs and Class Members have been injured by Microsoft's conduct, in the following, non-exhaustive ways:

a. they paid for a service or product advertised as having certain qualities as alleged above, when in fact the product did not have those qualities;

b. they paid more for a service or product advertised as having certain qualities as alleged above, when in fact the product did not have those qualities; and

c. their data has been placed at risk through Microsoft's use and sharing of it, and its noncompliance with SOC standards.

196. Under RCW 19.86.090, Plaintiffs and Class Members are entitled to:

a. a cease and desist order;

b. restitution;

c. actual damages;

d. treble damages;

e. costs; and

f. attorney fees.

Count Four
Violations of Washington Privacy Act
RCW §§ 9.73.010, et seq.
On behalf of Plaintiffs and the Class

197. Washington's Privacy Act, RCW. §§ 9.73.010, *et seq.*, prohibits the interception of a private communication transmitted by device between two or more individuals without first obtaining the consent of the participants in the communication. *Id.* § 9.73.030(1)(a).

198. Microsoft is not exempted from Privacy Act liability under RCW § 9.73.070.

199. Through its use and sharing of business customer data as alleged above, Microsoft has intercepted private communications in violation of RCW § 9.73.030(1)(a), without first obtaining the consent of the participants in the communications.

200. Microsoft obtained the content of Plaintiffs' and Class Members emails and other private communications, without consent.

201. Microsoft shared that content with unauthorized third parties, including software application developers and hundreds of subcontractors, who use the data for their own purposes, or for purposes that benefit Microsoft, without consent.

202. Microsoft used that content to glean business intelligence and develop new products—such as Microsoft Graph, Security Graph API, and Audience Network—to sell to others, and to improve products regardless of whether the business customer uses the product, without consent.

203. As alleged above, Plaintiffs and Class Members were injured in their business, person or reputation. Plaintiffs and Class Members paid for Microsoft's services, without knowledge or consent that Microsoft was using and sharing their private communications as alleged above.

204. Plaintiffs bring this claim based upon all allegations in this Amended Complaint, except the Facebook allegations in Part C.1.a.

205. Under RCW § 9.73.060, Plaintiffs and Class Members are entitled to:

a. actual damages;

b. liquidated damages at the rate of $100 per day for each violation, up to $1,000;

c. litigation costs; and

d. reasonable attorney fees.

Count Five
Violations of Washington Common Law
Intrusion Upon Seclusion
On behalf of Plaintiff Russo and the Class

206. By surreptitiously accessing, using, and/or sharing Plaintiff Russo's and Class Members' data, including their contents, Microsoft intentionally intruded upon Plaintiffs' private affairs.

207. By repeatedly and purposefully accessing, using, and/or sharing Plaintiff Russo's and Class Members' data for Microsoft's own commercial use, including developing new features, new software, or reducing its costs, Microsoft's intrusion was intentional.

208. Plaintiff Russo and Class Members did not consent to, authorize, or know of Microsoft's intrusions. Microsoft knew it lacked knowing consent to access, use, or share Plaintiff Russo's and Class Members' data.

209. Plaintiff Russo and Class Members had a legitimate subjective expectation of privacy in their data.

210. Plaintiff Russo and Class Members also had a reasonable objective expectation of privacy in their data.

211. Microsoft's pervasive and recurring intrusions would be highly offensive to a reasonable person.

212. Microsoft's conduct was highly offensive and outrageous to a reasonable person.

213. By simultaneously assuring Plaintiff Russo and Class Members that Microsoft would use their data only to provide the agreed-upon services while in fact using the data for its own purposes, Microsoft acted with deceit and disregard, reinforcing the offensive and outrageous nature of its intrusions.

214. Microsoft's deception was deliberately orchestrated to conceal its intrusions from Plaintiffs and Class Members.

215. Plaintiff Russo and Class Members have suffered extensive damages as a direct and proximate cause of Microsoft's intrusions into its private affairs.

216. Plaintiff Russo and Class Members are entitled to:

a. restitution of the profits unjustly obtained;

b. recovery of payments for Microsoft's services;

c. punitive damages;

d. interest; and

e. other damages for Microsoft's invasion of privacy.

PLAINTIFFS DEMAND A TRIAL BY JURY.

DATED: July 21, 2021

BAILEY & GLASSER, LLP

/s/Arthur H. Bryant
Arthur H. Bryant
Attorneys for Plaintiff

Complete counsel listing on Page 1